

1 RITA M. HAEUSLER (SBN 110574)
2 rita.haeusler@hugheshubbard.com
3 HANNAH A. BOGEN (SBN 324294)
4 hannah.bogen@hugheshubbard.com
5 HUGHES HUBBARD & REED LLP
6 1999 Avenue of the Stars, 9th Floor
7 Los Angeles, CA 90067-4620
8 Telephone: (213) 613-2800
9 Facsimile: (213) 613-2950

Attorneys for Applicants Path Network, Inc. and Tempest Hosting, LLC

8 NURY SIEKKINEN (PRO HAC VICE)
9 nury@zwillgen.com
10 ZWILLGEN PLLC
11 1900 M Street NW, Suite 250
12 Washington, DC 20036
13 Telephone: (202) 706-5229
14 Facsimile: (202) 706-5298

Attorneys for Respondent Discord Inc.

13
14 **UNITED STATES DISTRICT COURT**
15 **NORTHERN DISTRICT OF CALIFORNIA**

17 In Re *Ex Parte* Application of
18 Path Network, Inc. and Tempest Hosting,
19 LLC,
20 Applicants.

CASE NO. 3:23-MC-80148-PHK

[MAGISTRATE JUDGE PETER H. KANG]

JOINT SUPPLEMENTAL BRIEFING

Pursuant to the Court’s August 23, 2023 order, Applicants Path Network, Inc. (“Path”) and Tempest Hosting, LLC (“Tempest”) (collectively “Applicants”) and Respondent Discord Inc. (“Discord”; collectively, the “Parties”) submit joint briefing as follows:

I. Introduction

The Parties hereby incorporate the contents of the Introduction section of the Joint Supplemental Briefing filed on September 1, 2023 (the “9/1 Briefing”). (ECF No. 21 p.1.)

II. Notice

a. Applicants’ Statement

The plain language of 18 U.S.C. § 2705 states that the Court shall grant a party’s request for delayed disclosure of a subpoena if “there is reason to believe that [disclosure] may have an adverse result” including the “destruction of or tampering with evidence.” *See* 18 U.S.C. § 2705 subds. (a), (b). To date, no court in the Ninth Circuit or the Supreme Court has held that a 90-day non-disclosure order violates the First Amendment.

Here, Applicants’ request for a 90-day non-disclosure order is supported by statute. Given the severe risk of spoliation as recognized by the Canadian Court, issuance of a brief, 90-day non-disclosure order preventing Discord from disclosing the Discord Subpoena to Curtis Gervais (“Gervais”) would not run afoul of the First Amendment.

Unsurprisingly, the cases that Discord cites for the proposition that a 90-day non-disclosure order violates the First Amendment are not on point. (*See* 9/1 p. 3.) In those cases, the Court’s First Amendment concerns were based on non-disclosure orders that were indefinite, the prohibition on speech was all-encompassing, and spoliation was not at issue. (9/1 Briefing p. 3 (citing *Microsoft Corp. v. United States Dep’t of Just.*, 233 F. Supp. 3d 887, 905 (W.D. Wash. 2017) (holding that Microsoft stated a plausible claim that indefinite nondisclosure orders violated the First Amendment); *Facebook, Inc. v. Pepe*, 241 A.3d 248, 260–61 (D.C. 2020) (holding that non-disclosure order prohibiting Facebook from telling *anyone* about anticipated production did not survive strict scrutiny, especially where there was no risk of spoliation of evidence). In fact, *Pepe* actually supports issuance of a non-disclosure order under the circumstances of this case. *see id.* at 262-64 (“Strict scrutiny is applied to avoid the ‘substantial risk’ to First Amendment rights posed by the

1 approval of these orders, which are content-based prior restraints. In these cases, the compelling
 2 interest prong of strict scrutiny is generally satisfied where there is a ‘reason to believe’ disclosure
 3 would lead to the adverse consequences enumerated in § 2705(b). On the narrow-tailoring prong,
 4 orders that issue for an indefinite time period fail to satisfy strict scrutiny, but orders limiting
 5 disclosure for a defined time period have generally been upheld.”) (citations omitted)¹. As
 6 established here, there is reason to believe that if a non-disclosure order is not issued in this case,
 7 evidence will be destroyed. Applicants have made a strong showing of this, supported by
 8 Canadian Court Orders and multiple affidavits. (See ECF Nos. 1, 1-1, 1-2, 1-3, 21.)

9 Applicants’ proposed non-disclosure order does not violate the First Amendment and the
 10 Court should grant its request for an order prohibiting Discord from notifying Gervais of the
 11 Discord Subpoena for 90 days.

12 **b. Respondent’s Statement**

13 The issue is not whether Gervais is “entitled” to notice or whether notice is “necessary,”
 14 but rather whether this Court should silence Discord in derogation of its First Amendment right to
 15 speak to its users. Applicants acknowledge that their request for a nondisclosure order in this
 16 context is novel, admitting they have found no support for their position. Applicants borrow from
 17 criminal nondisclosure orders under Section 2705, but the justification for such an order
 18 disappears when the target already knows he is a target. *See In re Grand Jury Subpoena to*
 19 *Twitter, Inc.*, No. 3:17-MC-40-M-BN, 2017 WL 9287146, at *6 (N.D. Tex. Sept. 22, 2017). Here,
 20 as Applicants assert, Gervais knows they seek his data in connection with the Canadian action.

21 Applicants’ only justification for such an extraordinary order is their fear of spoliation. But
 22 any danger of spoliation post-notice is illusory as Discord has already preserved all responsive
 23 accounts. Accordingly, a nondisclosure order is unnecessary and would impermissibly infringe on
 24

25
 26 ¹ Contrary to Discord’s argument (9/1 Briefing p. 4), *Pepe* does not hold that “fear of spoliation is
 27 not sufficient to ‘curtail a subpoenaed party’s First Amendment rights.’” *Id.* at 264 (holding that
 28 in *Pepe*, any mention of spoliation risk was “speculative” and insufficient to support the issuance
 of an expansive non-disclosure order).

Discord’s First Amendment right to speak to its users without any justification.

At the same time, Applicants also put forth the curious argument that notice from Discord to Gervais is not necessary because Gervais already knows that his data is being collected in connection with the Canadian action. Though Discord’s right to speak to its users does not depend on whether the communication is “necessary,” a nondisclosure order is likewise unnecessary because Gervais already knows that Applicants are seeking his data from Discord. Applicants can’t have it both ways—either (1) Gervais does not know Applicants seek his records from Discord, requiring an order to keep him in the dark or (2) he does know and a gag order is useless.

III. The Stored Communications Act

a. Applicants’ Statement

i. Passwords are not Content

Discord cannot escape the *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1083-84 (N.D. Cal. 2015) holding that a username and password, even taken together, do not constitute “content” for purposes of implicating the Stored Communications Act (“SCA”).

Here, Discord’s attempts to distinguish the Wiretap Act and the SCA should be disregarded. (9/1 Briefing p. 6.) While the Wiretap Act concerns interception of live communications, 18 U.S. Code § 2711, the Stored Communications Act concerns collection of stored communications. 18 U.S. Code § 2701. *Both* statutes concern access to communications, and *Carrier IQ* applies here. Consistent with the court’s clear explanation in that case, Gervais and Roosen’s usernames and passwords do not implicate the “substance, purport, or meaning” of their communications, do not constitute content covered by the SCA, and the Court should order Discord to produce them. *Carrier IQ*, 78 F. Supp. 3d at 1083-84.²

² Both cases that Discord cites in support of its argument that passwords are content are out of Circuit and inapposite. (9/1 Briefing p. 6) (citing *In re Toft*, 453 B.R. 186 (Bankr. S.D.N.Y. 2011) (debtor in Germany denied access to emails in United States in part because request was contrary to United States public policy; no mention of passwords as content); *Bower v. Bower*, 808 F. Supp. 2d 348 (D. Mass. 2011) (custody dispute concerning subpoena for production of mother’s emails; no mention of passwords as content).)

Further, the fact that Discord’s passwords are “hashed” and “salted” does not change Discord’s obligation to produce them. (9/1 Briefing p. 6.) Contrary to Discord’s assertions, Applicants have reason to believe that the “hashed” and “salted” passwords can be reverted to plaintext but the Court need not address that now, as Gervais and Roosen’s passwords are not content and the Court should order that Discord produce them, even in “hashed” and “salted” form.

ii. Gervais Impliedly Consented to Disclosure of his Communications

As noted in *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal. 2021), “[t]he critical question with respect to implied consent is whether the parties...had adequate notice.” *Id.* (citations omitted).

Here, as detailed in Applicant’s initial briefing, Gervais was on notice that certain subsets of his Discord communications were ordered to be collected by the Canadian Court because he is a party to the Canadian Action. (9/1 Briefing p. 5.) Additionally, as discussed in Mr. Warren’s affidavit, Gervais provided Mr. Warren with access to his devices and accounts on numerous occasions, demonstrating both his awareness of the Canadian Court’s Orders and his implied consent to the collection of his data. (*Id.* (Citing ECF No. 1-2.)) Further, if taken at face value, Gervais’s own statements that, pursuant to the Canadian Court’s Orders, he has tried, but failed, to access his accounts evidence his implied consented to disclosure of his Discord communications and his notice of their ordered disclosure. (*See* ECF No. 1-2 (detailing Gervais’s attempt to access his LastPass account which contains over 417 sets of login credentials).

All of the cases that Discord cites for the proposition that Gervais’s consent cannot be implied are distinguishable from the facts here because in those cases, there was no evidence of consent whatsoever. (9/1 Briefing pp. 6-8) (citing *Negro v. Superior Ct.*, 230 Cal. App. 4th 879, 893, 179 Cal. Rptr. 3d 215, 225 (2014), *as modified* (Nov. 18, 2014) (“The court cited no evidence, and there appears to have been no evidence before it, that Negro had in fact consented to disclosure...”); *Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726, 731 (9th Cir. 2011) (despite Australian order requiring him to produce documents, subscriber “vigorously argue[d]” against consent and “consistently objected to disclosure” of his communications); *Bower v. Bower*, 808 F.

1 Supp. 2d 348, 350–51 (D. Mass. 2011) (“[T]here is nothing in El–Nady’s actions from which this
 2 court can imply an intent to consent to the disclosure of her information.”); *Commonwealth v.*
 3 *Augustine*, 4 N.E.3d 846, 852 (Mass. 2014) (motion to suppress appeal with no discussion of
 4 implied consent at all); *see U.S. v. Councilman*, 418 F.3d 67, 75–76 (1st Cir. 2005) (appeal of
 5 motion to dismiss indictment for violation of Wiretap Act based on access to stored
 6 communications – no discussion of implied consent).)

7 Here, as specified in the Application, the 9/1 Briefing, and above, there is ample evidence
 8 that Gervais was on notice of the disclosure of his Discord communications and impliedly
 9 consented to their collection. Accordingly, the Court should order that Discord produce his
 10 communications.

11 **b. Respondent’s Statement**

12 **i. Passwords**

13 Applicants’ demand for passwords runs afoul of the SCA’s robust protection of the
 14 contents of electronic communications and would defeat the purpose of the law. *Bower v. Bower*,
 15 808 F. Supp. 2d 348, 350 (D. Mass. 2011) (SCA created a “zone of privacy” around the contents
 16 of communications). Applicants acknowledge that the SCA prohibits the disclosure of contents
 17 but urge that it does not prohibit providers from giving access to contents through disclosing
 18 passwords—the keys to all account contents. Incredibly, Applicants assert that passwords “do not
 19 implicate” the contents of electronic communications. DKT. 21 at 6. If not to access the contents
 20 of the target accounts, it is difficult to imagine why Applicants seek passwords.

21 Applicants present no cases holding that the disclosure of passwords in response to a
 22 subpoena is consistent with 18 U.S.C. §2702. Instead, Applicants entire argument relies on one: *In*
 23 *re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1060 (N.D. Cal. 2015). That court held that software on
 24 cellphones that allegedly intercepted a variety of information including passwords did not violate
 25 the Wiretap Act—it did not address the SCA. However, there is no indication in the opinion that
 26 any entity or person was intercepting the passwords *for the purpose of accessing content*. On the
 27 contrary, the allegations indicate that the software ran in the background as a network diagnostic
 28 tool. *Id.* at 1061–62. In that context, the passwords intercepted do not implicate the extreme

1 privacy concern of third parties acquiring digital passwords via subpoena for the purpose of
2 accessing contents.

3 In any event, the question of whether Discord may be ordered to produce a user's
4 passwords is academic because Discord stores only the "hashed" and "salted" values of user
5 passwords as a security feature.

6 **ii. Gervais's Consent**

7 Applicants fail to cite any cases holding that a user has consented to disclosure under the
8 circumstances presented here, likely because the case law weighs heavily against finding consent
9 where there is no express consent to the provider's disclosure of content. Indeed, Applicants' lone
10 citation on this issue is to *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal. 2021),
11 which supports Discord's position. *Calhoun* acknowledges that "the party seeking the benefit of
12 the exception" has the "burden to prove consent." *Id.* Moreover, consent must be "actual" and any
13 consent based on disclosures by the provider "must explicitly notify the users of the practice at
14 issue." *Id.* (citing *In re Google, Inc.*, 2013 WL 5423918, at *12-13 (N.D. Cal. Sept. 26, 2013)).
15 Here, Applicants have not carried their burden because the Application reveals Gervais's
16 obstruction, not his consent to Discord's disclosure of content. In addition, there have been no
17 disclosures by Discord like those in *Calhoun* and certainly no disclosures to Gervais explicitly
18 notifying him that Applicants seek the data directly from Discord. Even if there had been such
19 disclosure,³ case law on civil subpoenas and the SCA uniformly hold that notice alone or notice
20 plus inaction or obstruction do not support a finding of consent. *Suzlon Energy Ltd. v. Microsoft*
21 *Corp.*, 671 F.3d 726 (9th Cir. 2011); *Negro v. Superior Ct.*, 230 Cal. App. 4th 879, 889, 179 Cal.
22 Rptr. 3d 215, 222 (2014), *as modified* (Nov. 18, 2014). Constructive consent or consent assumed
23 based on constructive notice (*see* DKT 21 at 3 (no SCA violation because "Gervais was on
24 notice")) is not actual, lawful consent-in-fact required by the SCA.

25 The Warren Affidavit cannot support a finding of consent. At best, the Warren Affidavit
26

27
28 ³ Indeed, Applicants argue vigorously against any such disclosure by Discord.

shows that Gervais consented to Warren’s very limited search of some of his devices but did not consent to Warren searching many of his online accounts, including his Discord account. *See* DKT1-2 at 3, 5, 8, 11-13. Indeed, the fact that applicants were not able to acquire Gervais’ Discord password and contents via his alleged “consent” and is now seeking it from Discord through this 1782 application demonstrates that Gervais he has not consented.

IV. Litigation Hold

a. Applicants’ Statement

Discord is required under *Apple Inc. v. Samsung Elecs. Co.*, 888 F. Supp. 2d 976, 991–92 (N.D. Cal. 2012) to halt all routine deletion procedures with respect to Gervais’s and Roosen’s accounts because litigation is reasonably anticipated. *Id.*; *see also See In re Napster, Inc. Copyright Litig.*, 462 F. Supp. 2d 1060, 1069 (N.D. Cal. 2006) (applying preservation obligations to third party). Without doing so, Discord has not met its preservation obligations. *Id.*

Contrary to Discord’s assertions, Applicants are not asking that the Court order Discord to pause its deletion procedures or capture future data indefinitely. (9/1 Briefing p. 8.) Applicants only ask that the Court order Discord to do what it is required under *Samsung* - halt all routine deletion procedures until documents subject to the Discord Subpoena have been produced. 888 F. Supp. 2d at–92.⁴

b. Respondent’s Statement

Applicants’ argument concerning what they term a “litigation hold” appears to be based on a fundamental misconception—they appear to contend Discord’s routine deletion practices will delete the data preserved from the accounts at issue here. Indeed, Applicants assert that Discord “did not” halt routine data deletion with respect to the preserved accounts. This is not so. As

⁴ Discord’s argument that two preservation snapshots – one on or around August 17, 2023 and one at the time of production, are sufficient to satisfy its preservation obligations is plainly incorrect. (9/1 Briefing p. 8.) If Gervais or Roosen engage in further communications, create new aliases, or otherwise, between August 17, 2023 and the time of production, and Discord’s routine deletion procedures are not halted, evidence of those communications and aliases could be lost forever. It is for that reason that courts like that in *Samsung* require a pause on routine deletion procedures when litigation is reasonably anticipated. 888 F. Supp. 2d at 991-92.

Discord does under Section 2703(f), the snapshots Discord has already preserved in this matter *are not* subject to routine deletion of data.

In re Napster is inapposite as there is no indication that Discord will be sued in the underlying litigation. In any event, Discord has already preserved the responsive accounts such that ordinary record retention policies or user-instigated changes will not affect the preservations. None of Applicants' cases indicates that Discord—a third-party subpoena respondent unconnected to any of the underlying litigants—has an obligation to preserve data that is yet to be created.

Respectfully submitted,

DATED: September 8, 2023

RITA M. HAEUSLER
HANNAH A. BOGEN
HUGHES HUBBARD AND REED LLP

By: /s/ Hannah A. Bogen

Hannah A. Bogen
Attorneys for Applicants
PATH NETWORK, INC. AND
TEMPEST HOSTING, LLC

DATED: September 8, 2023

NURY M. SIEKKINEN
ZWILLGEN PLLC

By: /s/ Nury M. Siekkinen

Nury M. Siekkinen
Attorneys for Respondent
DISCORD, INC.